REMARKS

Claims 1-19 were pending prior to this amendment. Claims 1-19 have been rejected. Claims 1, 4-7, 12, 15 and 17 have been amended. New claims 20-24 have been added. Applicant respectfully requests reconsideration and allowance of all pending claims.

Drawing Objections

The drawings have been objected to.

Applicant has included formal drawings according to the recommendation made by the Examiner.

Claim Rejections – 35 U.S.C. § 112

Claims 4-7, 12 and 15 stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 4-7 and 15 have amended to correct typographical errors.

Claim 12 has been amended for clarification.

Claim Rejections – 35 U.S.C. § 102

Claims 1-3 stand rejected under 35 U.S.C. §102(b) as being clearly anticipated by both U.S. Patent No. 5,991,292 to Focsaneanu, et al. and U.S. Patent No. 6,137,869 to Voit, et al.

Claim 1 has been amended. Applicants claim receiving packets with encrypted layer four transport layer headers and encrypted payloads and then replacing layer three network layer headers included in those packets all while preserving encryption protecting the media. This feature is usable for transferring encrypted media between packet switched and circuit switched networks without requiring intermediary decryption. This is described in the present specification, at least paragraph 32.

Focsaneanu does not teach this feature. Information in Focsaneaunu is not transferred between a circuit switched network and a packet switched network without decryption.

Voit does not teach this feature. Information in Voit is not transferred between a circuit switched network and a packet switched network without decryption.

With respect to Edgett, even if it was obvious at the time of filing the present application to modify Focsaneanu or Voit with Edgett (which it was not), the alleged combination would still fail to teach the claimed features.

Referring to FIG. 2 of Edgett and the accompanying text, Edgett discloses password encryption. An endpoint encrypts a password, transfers the encrypted password over the PSTN to a NAS 220. The NAS 220 forwards the encrypted password to Authentication System 265 for decryption. Accordingly, Edgett does not teach the feature of formatting a layer three header while preserving encryption on a layer four header and an encompassed payload.

In contrast, claim 1 includes the feature of formatting a layer three network layer header while preserving encryption on a layer four transport layer header and an encompassed payload. Thus, claim 1 should be allowed. Claims 2-3 are dependant and should also be allowed.

Claims 5, and 17 stand rejected under 35 U.S.C. §102(b) as being clearly anticipated by U.S. Patent No. 6,137,869 to Voit, et al.

Claim 5 is dependent and should be allowed for at least the same reason as claim 1. Independent claim 17 has been amended and should be allowed for at least the same reason as claim 1.

Claim Rejections – 35 U.S.C. § 103

Claims 4, 10, and 11 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,137,869 to Voit as applied above, and further in view of U.S. Patent Application Publication No. 2003/0056092 to Edgett, et al.

No amendments have been made to claim 10. None of the references disclose transferring an encrypted IP packet payload over a circuit switched network and a packet switched network without intermediary decryption. An encrypted IP packet payload is usable for sending voice or video over a circuit switched network and a packet switched network efficiently and securely. None of the references teach this feature.

Voit does not disclose the claimed feature. This was acknowledged in the Office Action on page 6 of the Office Action.

Edgett discloses an endpoint encrypting a password using the Password Authentication Protocol (PAP). *See* paragraph 68. The PAP protocol and other handshaking protocols that function similarly are not the same or even analogous to the claimed IP packet

payload. For example, the PAP protocol and similar authentication protocols cannot be used to transfer voice data and/or video using a payload. In other words, not only is the PAP packet simply not the same as the claimed IP packet payload, the two have substantial functional differences. Thus, Edgett fails to disclose at least the element of transferring an encrypted IP packet payload over a circuit switched network and a packet switched network without intermediary decryption. As a result the alleged combination is unable to transfer voice or video over a circuit switched network and a packet switched network without intermediary decryption.

In contrast, claimed feature includes an encrypted IP packet payload that is transferred from one endpoint to another over a circuit switched network and a packet switched network without intermediary decryption. This feature is usable to transfer media such as video and voice data securely and efficiently without intermediary decryption at a PSTN gateway. Thus, claim 10 should be allowed. Claims 4 and 11 are dependent and should be allowed for at least similar reasons.

Claims 6, 7, and 18 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,137,869 to Voit as applied above, and in view of U.S. Patent No. 5,392,357 to Bulfer.

Claims 6, 7 and 18 are dependent and should be allowed for at least the same reason as their respective parent claims.

Claim 8 stands rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,137,869 to Voit.

Claim 8 is dependent and should be allowed for at least the same reason its parent claim.

Claim 9 stands rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,137,869 to Voit as applied above, and in view of U.S. Patent Application Publication No. 2004/0019801 to Lindholm, et al.

Claim 9 is dependent and should be allowed for at least the same reason its parent claim.

Claim 19 stands rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,137,869 to Voit in view of U.S. Patent No. 5,392,357 to Bulfer as applied above, and further in view of Bruce Schneier's *Applied Cryptography* (2nd edition).

Claim 19 is dependent and should be allowed for at least the same reason its parent claim.

Claims 4, 10, and 11 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,991,292 to Focsaneanu, et al in view of Edgett.

No amendments have been made to claim 10. None of the references teach transferring an encrypted IP packet payload over a circuit switched network and a packet switched network without intermediary decryption.

Focsaneanu does not disclose the claimed feature. Rather, traffic is decrypted during transferring.

Improving Focsaneanu with Edgett, if it were possible, still does not teach the claimed feature. Edgett teaches inserting a password into a field of an encrypted PAP packet or a functionally equivalent packet. *See* FIG. 2 and paragraph 68. Adding such a feature to Focsaneanu would only allow encrypted password exchange, which is not the same as transferring an encrypted IP packet payload over a circuit switched network and a packet switched network without intermediary decryption.

In contrast, the claimed feature includes an encrypted IP packet payload that is transferred from one endpoint to another over a circuit switched network and a packet switched network without intermediary decryption. This feature is usable to transfer video and voice data securely and efficiently without intermediary decryption at a PSTN gateway. Thus, claim 10 should be allowed. Claims 4 and 11 are dependent and should be allowed for at least the same reasons as their respective parent claims.

Claim 9 stands rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,991,292 to Focsaneanu, et al. as applied above and in view of U.S. Patent Application Publication No. 2004/0019801 to Lindholm, et al.

Claim 9 is dependent and should be allowed for at least the same reason its parent claim.

Claim 12 stands rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,991,292 to Focsaneanu, et al. and in view of U.S. Patent Application Publication

No. 2003/0056092 to Edgett, et al. as applied above, and further in view of U.S. Patent Application Publication No. 2005/0125357 to Saadat, et al.

Claim 12 is dependent and should be allowed for at least the same reason its parent claim.

Claim 13 stands rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,991,292 to Focsaneanu, et al. and in view of U.S. Patent Application Publication No. 2003/0056092 to Edgett, et al. as applied above, and further in view of U.S. Patent No. 6,426,948.

Claim 13 is dependent and should be allowed for at least the same reason its parent claim.

Claim 14 stands rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,991,292 to Focsaneanu, et al. and in view of U.S. Patent Application Publication No. 2003/0056092 to Edgett, et al. as applied above, and further in view Bruce Schneier's *Applied Cryptography* (2nd edition).

No amendments have been made to claim 14. The Office Action regards the claimed subject matter as only specifying encrypting a first key using a shared key. *See* page 14, last paragraph. However, the claim 14 specifies the additional limitation that the shared key is shared with "an ingress device located at an ingress side of the IP network." This additional limitation was not addressed by the Office Action.

Schneier does not disclose encryption of a first key with a shared key that is share with an ingress device located at an ingress side of the IP network. Alice and Bob's public keys are shared with a remote database located on a packet switched network. The remote database is not an ingress device located at an ingress side of the network. There is no suggestion in Schneier or any of the cited references for the network processing device to encrypt a first key with a shared key that is shared with an ingress device located at an ingress side of the IP network.

In contrast, claim 14 encrypting a first key using a shared key that is shared with an ingress device located at an ingress side of the IP network. This is shown, for example, in FIG. 1 of the present application where both gateways 16 and 26 are preconfigured out of band with a shared secret. Thus, claim 14 should be allowed. New claim 24 has been added.

Claim 15 stands rejected under 35 U.S.C. §03(a) as being unpatentable over U.S. Patent No. 5,991,292 to Focsaneanu, et al. and in view of U.S. Patent Application Publication No. 2003/0056092 to Edgett, et al. and Bruce Schneier's *Applied Cryptography* (2nd edition), and further in view of U.S. Patent No. 5,392,357 to Bulfer.

Claim 15 is dependent and should be allowed for at least the same reason its parent claim.

Claim 16 stands rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,991,292 to Focsaneanu, et al. and in view of U.S. Patent Application Publication No. 2003/0056092 to Edgett, et al. as applied above, and further in view of U.S. Patent Application Publication No. 2004/0019801 to Lindholm.

Claim 16 is dependent and should be allowed for at least the same reason its parent claim.

New Claims

New claims 20-23 have been added. Support for the new claims may be found in the present specification, at least paragraph 32.

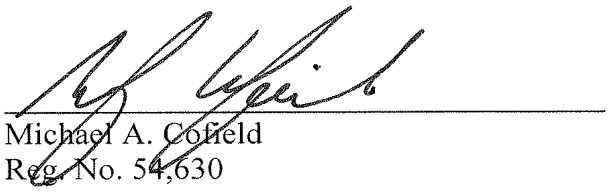
New claim 24 has been added. Support for the new claim may be found in the present specification, at least paragraphs 18 and 21.

CONCLUSION

For the foregoing reasons, reconsideration and allowance of all pending claims is requested. The Examiner is encouraged to telephone the undersigned at 503-222-3613 if it appears that an interview would be helpful in advancing the case.

Respectfully submitted,

MARGER JOHNSON & McCOLLOM, P.C.



Michael A. Cofield
Reg. No. 54,630

MARGER JOHNSON & McCOLLOM, P.C.
210 SW Morrison Street, Suite 400
Portland, OR 97204
503-222-3613
Customer No. 20575